Spotlight On: Insider Threat from Trusted Business Partners

Version 2: Updated and Revised

Todd Lewellen
Andrew P. Moore
Dawn M. Cappelli
Randall F. Trzeciak
Derrick Spooner
Robert M. Weiland

October 2012

This work was funded by

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2012		

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Spotlight On: Insider Threat from Trusted Business Partners. Version 2: Updated and Revised	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University ,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**18**	

This material is based upon work supported by the United States Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the

Contracting Officer
ESC/CAA
20 Shilling Circle
Building 1305, 3rd Floor
Hanscom AFB, MA 01731-2125

Table of Contents

Introduction

This article is the sixth in the series *Spotlight On*, published by the CERT® Insider Threat Center at Carnegie Mellon University's Software Engineering Institute and funded by CyLab. Each article focuses on a specific area of concern and presents analysis based on hundreds of actual insider threat cases cataloged in the CERT insider threat database. For more information about the CERT Program's insider threat work, see http://www.cert.org/insider_threat/.

This article focuses on cases in which the malicious insider was employed by a trusted business partner of the victim organization. We first define the concept of trusted business partner (TBP) and then describe case scenarios in which a TBP has become an insider threat. These case scenarios concentrate on presenting the *who*, *what*, *why*, and *how* of the illicit activity. Finally, we provide recommendations that may be useful in countering these threats.

We would like to thank the following for their contributions to this article: Sally Cunningham, deputy director, Program Development and Transition at the SEI; William Shore, retired special agent with the FBI who is now the manager of security at the Software Engineering Institute; and Dr. Eric Shaw, an independent contractor at the CERT Program and clinical psychologist at Consulting & Clinical Psychology, Ltd.

Snapshot of Insider Threat from Trusted Business Partners

What Is a Trusted Business Partner?

For the purposes of this article, a ***trusted business partner*** (TBP) is defined as any external organization or individual an organization has contracted to perform a service for the organization. The nature of this service requires the organization to provide the TBP authorized access to proprietary data, critical files, or internal infrastructure. For example, if an organization creates a contract with an outside organization to perform billing services, it would have to provide access to its customer data, thereby establishing a trusted business partnership. However, the TBP concept does not include cases in which the organization is simply a customer of another company. For example, when an organization uses a bank, it is simply a client of the bank. This customer-vendor relationship would not be considered a TBP relationship.

This definition includes two different types of relationships between the organization and the TBP. An ***organizational relationship*** is one in which one organization outsources a service to a TBP. For example, an organization outsourcing its customer helpdesk service to an outside company has entered into a TBP relationship with that company. In this case, the organization must grant access to its customer database to the outside organization.

® CERT is a registered mark owned by Carnegie Mellon University.

In contrast, some employees working for a TBP could have an individual relationship with the victim organization. An ***individual relationship*** includes individual consultants, temporary employees, and contracted employees. An ***individual consultant*** is an individual who performs services for the organization but is not an employee of the organization. This includes any employees who have terminated their employment with an organization and who are then hired on as consultants. A ***contracted employee*** is any employee hired under a contractual agreement between an organization and a contract organization (the TBP). The contracted employee works full time for the organization but receives compensation from the TBP. A ***temporary employee*** is any person hired for a short period of time, for example, to fill a seasonal need or a position left open by an employee who has departed or gone on leave.

Overview of Insiders from TBPs

According to a study that surveyed C-level executives, conducted in 2009 by the security companies RSA and Interactive Data Corporation (IDC), "Contractors and temporary staff represent the greatest internal risk [to] organizations" [Burke 2009]. However, of the more than 575 cases in the CERT MERIT database,[1] only 50 were committed by contractors, consultants, or temporary staff, accounting for roughly 8.7% of all cases. So, while the RSA/IDC survey indicates the problem of attacks by contractors and temporary staff is of high concern to the C-level executives surveyed, our data shows that individuals employed directly by an organization were more often the perpetrators of insider crimes than contractors or temporary staff.

TBP insider cases occurred in a number of industry sectors. For example, while a greater number of cases occurred in the government and information technology sectors, cases were also observed in the financial, medical, education, entertainment, manufacturing, and utility sectors. Figure 1 below displays the breakdown of cases by industry according to the cases in the CERT insider threat database.

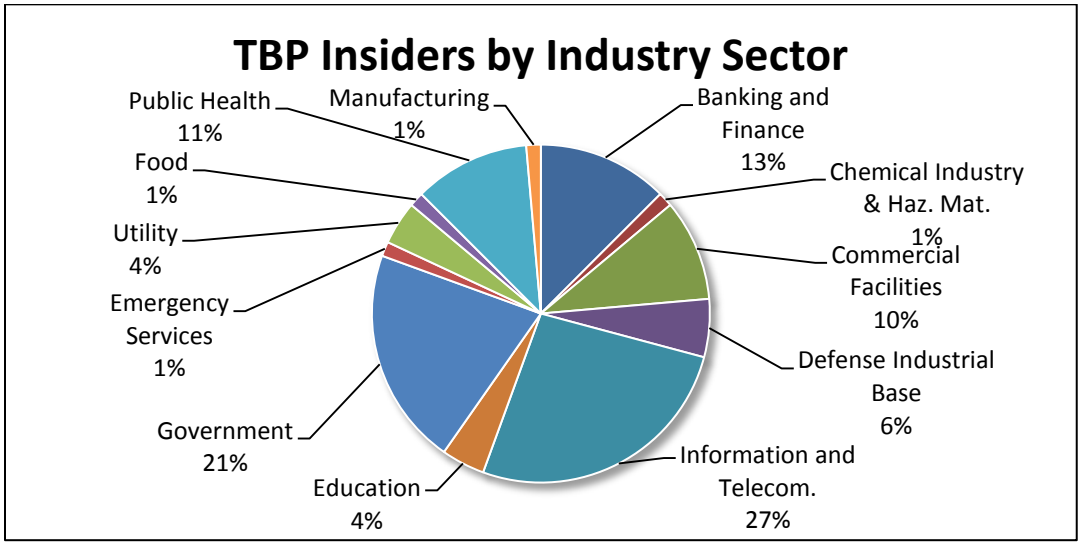

Figure 1: TBP Insiders by Industry Sector

[1] At the time of writing, there are 578 cases in the MERIT database. These cases specifically include incidents of IT sabotage, fraud, and theft of intellectual property (IP), as well as a small subset of cases that do not fit into those three categories. They do not include the 120 espionage cases we have also researched.

In addition to the 50 cases involving contractors, consultants, and temporary employees (which fall under the definition of TBPs with an individual relationship), there were 25 cases involving TBPs in an organizational relationship with victim organizations (Figure 2).

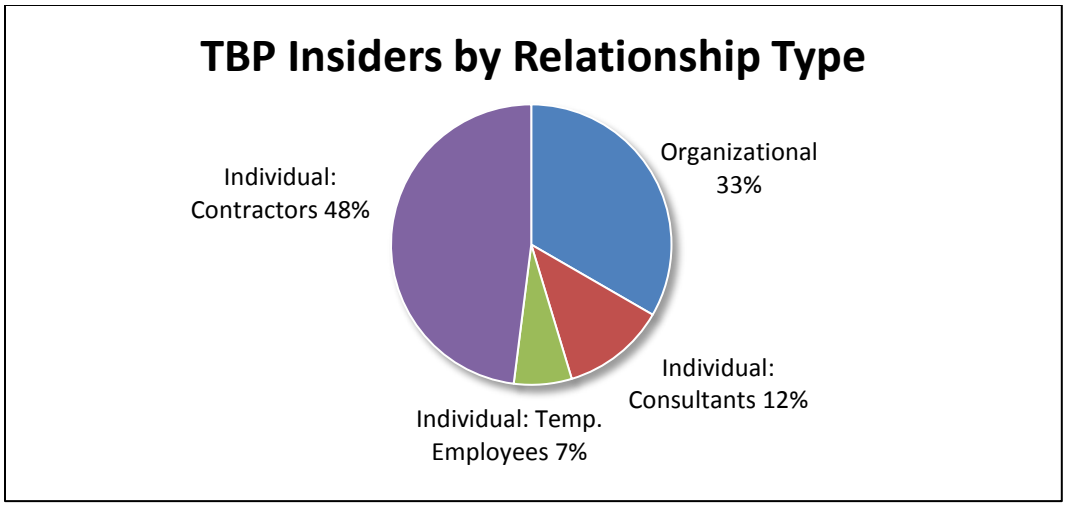

Figure 2: TBP Insiders by Relationship Type

Organizations may form a relationship with a TBP to satisfy diverse needs. For instance, the organization might need employees for either technical or nontechnical positions. ***Technical positions*** include any information technology job requiring specialized computer skills or technical knowledge, such as software development, network administration, and system administration, as well as engineering and scientific research. ***Nontechnical positions*** include any job that does not require specialized computer skills or technical knowledge, such as jobs in data processing, facilities services, or claims processing.

Figure 3 shows the number of cases observed for each type of insider crime classified by employee type: technical or nontechnical. The figure clearly shows nontechnical TBP insiders were more likely to commit fraud, while technical TBP insiders were more likely to commit IT sabotage and steal intellectual property (IP).

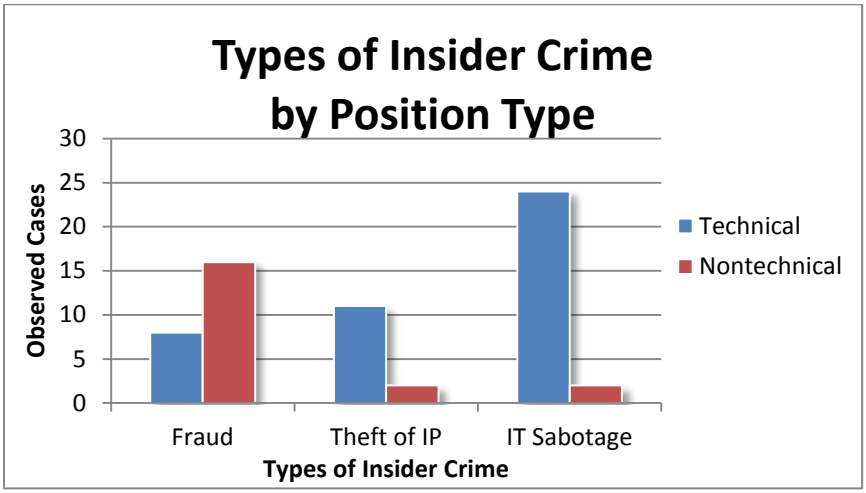

Figure 3: Types of TBP Insider Crime Based on Position Type (Technical/Nontechnical)

Figure 4 presents the number of TBP insiders for each type of relationship (organizational or individual) combined with the type of position held (technical or nontechnical). From this analysis, two categories emerge with larger distinct patterns of insider crime. Regardless of their type of relationship with the victim organization, nontechnical TBPs were far more likely to commit fraud than steal IP or commit sabotage. Of the technical TBPs with individual relationships with their victim organizations, two-thirds committed sabotage. Across all cases involving TBP insiders, most crimes were committed by males (84%), which is slightly more than non-TBP insider cases (68%).

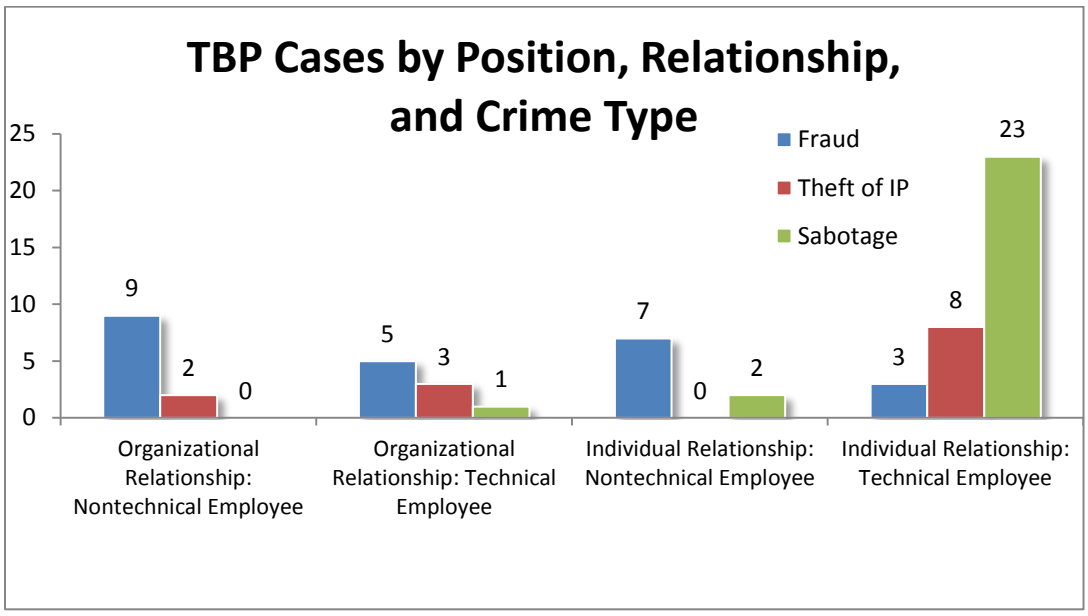

Figure 4: TBP Cases by Type of Position and Relationship of TBP Insider with the Victim Organization

Figure 5 shows the age distribution of TBP and non-TBP insiders and compares it against the age distribution of the 2010 U.S. labor force [U.S. Census Bureau 2011]. The trend shows that the average insider is slightly younger than the average working American, and that TBP insiders are at their greatest risk of committing a malicious act between the ages of 25 and 34.

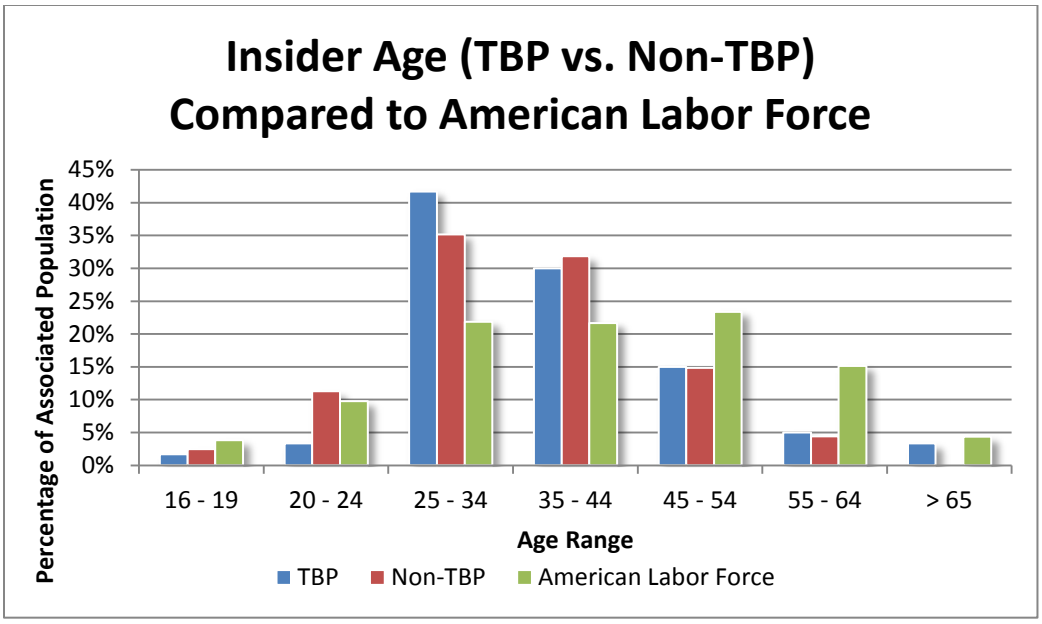

Figure 5: Comparison of TBP and Non-TBP Insiders against American Labor Force

TBP Insider Case Scenarios and Analyses

Scenario I: TBP Insiders with an Organizational Relationship

The following scenario is based on a typical case of a TBP insider with an organizational relationship with the victim organization. The insider used her access to commit fraud and extort thousands of dollars from the victim organization.

The insider worked for a TBP that formed a relationship with another organization to handle claims processing. The organization provided the TBP with 10 authorized accounts and a VPN tunnel into its network, which could be used from the TBP's remote location. The authorized accounts were able to process claims, add accounts, and modify account details for the organization's clients. The insider processed claims each day for a number of months and became very familiar with the organization's system and its audit controls. The insider realized that when claims are expedited no secondary approval is required to settle the claim and mail a disbursement check.

As a claims processer, the insider did not make much money, and she struggled to pay all of her bills on time. She told her boyfriend about the expedited service, and he convinced her to expedite a claim in his name to try it out. The insider created a fake claim, and a disbursement check was sent to her boyfriend. He cashed the check and they shared the money.

The insider became a bit nervous at work and wondered if anyone knew about what she had done. After a couple of weeks, no one approached her and she assumed it was not likely anyone had noticed her actions. Emboldened, she decided to create another expedited claim, and another check arrived at her boyfriend's house. The insider and her boyfriend decided suspicions might be

aroused if too many claims were filed against one account, so her boyfriend convinced her to expedite and approve claims for his friends. He proposed they split the money with his friends when they cashed the checks.

The insider proceeded to make false claims, and she and her boyfriend were able to recruit a number of friends to help them perpetrate their scheme. Several months later, during a routine audit, a manager at the victim organization noticed an unusually high number of expedited claims were processed using one of the accounts provided to the TBP. The victim organization was able to trace the activity to the TBP insider and shut down the operation. In all, the insider expedited more than 60 false claims with amounts ranging from $100 to $1,500, costing the company more than $75,000.

Analysis

This is an example of the types of insider crimes that occur with a TBP in an organizational relationship. As noted, organizational relationships arise when an organization outsources a service to a TBP. This case demonstrates what can go wrong when an organization provides a TBP with authorized but unsupervised access. In this case, the insider was not technical; she learned how to commit the fraud simply by observing the claims process.

Examining the cases of TBP insiders in organizational relationships documented in the CERT insider threat database, we found that the majority of observed insiders had authorized access to the systems exploited. All but 10% were currently employed by the TBP organization and working at the victim organization at the time of the incident, and 81% conducted their attack on-site. Slightly over half of them (55%) held nontechnical positions. Interestingly, the average impact of insiders in organizational relationships was greater than that of insiders in individual relationships. For example, one case involved a helpdesk employee who created a fake email address to order parts to be sold on eBay, costing the victim organization $4.7 million. Overall, for the 23[2] organizational relationship cases for which we have data, the average loss was $930,000 and the median loss was $15,000.

Nontechnical insiders are typically assigned tasks that use IT resources to process customer or employee data. Additionally, nontechnical insiders tend to be in lower level positions. These factors partially account for why nontechnical insiders typically exploit the victim organization for financial gain through fraud.[3] Nontechnical TBP insiders with an organizational relationship were more likely to commit fraud (64%) than theft of IP[4] (28%) or sabotage (8%).

---

[2] Out of the 27 organizational TBP cases in our database, 3 had unknown monetary damages and 1 case had an outlier damage amount of $100 million.

[3] ***Insider Fraud*** occurs when an insider uses IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or to otherwise facilitate an *identity crime*. This includes theft and sale of confidential information (for instance social security and credit card numbers), modification of critical data for pay (such as driver's license records, criminal records, and welfare status), and theft of money (from financial institutions, government organizations, etc.). ***Identity crime*** is "the misuse of personal or financial identifiers to gain something of value and/or facilitate other criminal activity" [U.S. Secret Service].

[4] ***Theft of intellectual property*** is an insider's use of IT to steal *intellectual property* from the organization. ***Intellectual property (IP)*** is a term referring to original creative thoughts, which include proprietary information

Case Summaries: TBP Insiders with Organizational Relationships

In the sample cases summarized below, the insider worked for the TBP and had an organizational relationship with the victim organization.

1. The insider was a claims processor at the TBP, which had an organizational relationship with an insurance company. The insider used authorized access to divert millions of dollars through falsified insurance claims to a personal address. The insider got away with the crime because there was no system in place to double check the edited claims.
2. The insider colluded with a fellow employee while working as customer support representatives for a TBP that had an organizational relationship with a state government agency. The insiders manipulated state benefit transactions to fraudulently receive $32,000 in food stamp kickbacks and issue food stamps to people who did not qualify. The beneficiaries would pay the insiders with part of the illicit funds they received. The insiders found a flaw that allowed expedited cases to be approved without supervisor authorization. They were caught when the supervisor reviewed records and discovered the illegal activity.
3. Two insiders were employed as engineers at a tire equipment manufacturing company. Their organization had acquired a contract with a Chinese company to manufacture a piece of equipment that the insiders were struggling to design. The victim organization, a previous client of the insiders' organization, had already developed a proprietary version of the equipment that the Chinese company desired. The insiders scheduled a visit to the victim's manufacturing plant under the pretense of inspecting their own organization's equipment for potential repairs. While one insider kept a lookout, the other insider used the camera on his cell phone to take several pictures of the victim's proprietary equipment and email them back to his fellow employees.
4. The insider was employed as a computer helpdesk agent at a TBP performing computer support for a government organization. The insider created an unauthorized email address and used it to have replacement parts sent to his home. He sold the parts on eBay. The insider made over half a million dollars on the sale of more than 90 parts.
5. The insider was a student who was unofficially working for his uncle. The uncle worked for a document imaging company that was subcontracted by an outside law firm working for the victim organization, a telecommunications company. The insider stole trade secret information and posted it online. When the post was discovered, the FBI investigated the source of the trade secrets posted to the internet and traced the activity back to the student.
6. The insider was employed as a computer engineer by a TBP that managed computer systems for the victim organization, a foreign government. One month prior to the incident, the insider resigned from the TBP due to stress and disagreements with his employer. At the time, the insider was living with a former colleague, who was still employed by the TBP organization. The insider used his colleague's work computer and credentials to open a VPN connection, shut down multiple government servers, and

---

such as patents, copyright material, trademarks, engineering designs and scientific formulas, proprietary source code, and confidential customer information; however, it does not include identity crimes [Moore 2009].

delete thousands of accounts for government employees at the victim organization. Though the insider claimed he was trying to expose security vulnerabilities in the government's IT systems, he was arrested and convicted for causing approximately $1.2 million in damages.

Scenario II: TBP Insiders with an Individual Relationship

The following scenario is based on a typical case of a TBP insider with an individual relationship with the victim organization. The insider used his authorized access and privileges to commit IT sabotage against the victim organization.

An organization received a resignation notice from its long-time systems administrator. The small organization did not have a second administrator on staff to promote, so it had to quickly hire a contractor to fill the position before the current administrator left the company.

The contractor worked with the outgoing systems administrator for the last month of his employment. The organization told the contractor he was being groomed to fill the position and would be hired on full time when his 6-month contract ended.

About 3 months into the contract, the contractor started showing up late. When a manager discussed this with the contractor, the contractor became very disturbed and threatened the manager. After lengthy discussions, the organization decided it should look for someone else to take on the full-time position.

About a month before the contract was set to end, the organization hired a new systems administrator and asked the contractor to train him. The organization informed the contractor he would not be continuing full time as previously hoped. The contractor became resentful and set up a fake account with administrative privileges to the network.

He remotely logged into the company using the fake account and planted a logic bomb set to launch malware that could have crippled the company's network and systems. The logic bomb was set to launch a week after his dismissal. Fortunately, the new administrator discovered the rogue account when reviewing the remote access logs. He also discovered the malicious code before it was executed and was able to trace the source of the remote login to a specific IP address. Law enforcement traced the IP address to the contractor's father's home.

Analysis

This case is an example of a TBP insider in an individual relationship with the victim organization, and it demonstrates how providing privileged, authorized access to a contractor can backfire, as well as the risks associated with allowing such individuals to remain on-site when they become disgruntled. It also demonstrates how a technical employee could have the knowledge to create back-door access into a system and plant malicious code capable of causing a great deal of harm to the organization.

In the cases of TBP insiders with individual relationships documented in the CERT insider threat database, the distinguishing characteristic was the insider's technical role. In 45 of the 50 cases of TBPs with individual relationships, we were able to determine the insider's role (technical or

nontechnical). The majority held technical positions (36) as opposed to nontechnical positions (9). To carry out their attacks, half of these individuals used an unauthorized means of access to the organizations' systems, such as an account that should have been disabled after termination, a back-door account, or another employee's account. The exploits by technical TBP insiders occurred both on-site (60%) and remotely (40%). Of the cases in which the insiders attacked the victim location on-site, the large majority occurred during work hours. Slightly more than half of the insiders who perpetrated remote exploits of the victim organization did so outside of normal business hours.

When compared with those in organizational relationships, TBPs in individual relationships tended to cause less damage during the course of their attacks. The average cost of an attack from a TBP with an individual relationship was $177,000. However, the median loss, $25,000, was slightly greater than that of organizational TBPs.

Technical insiders held positions that provided them with elevated access to the victim organization. Insiders in technical positions typically found vulnerabilities in the victim organization and used their technical knowledge to exploit them.

Revenge was the primary motivating factor in cases involving insiders with individual relationships. It played a significant role in nearly half of the cases (46%), whose objective was IT sabotage.[5] These individual TBP insiders sought revenge for not being offered full-time employment with the victim organization, for not having their contract renewed, for not receiving a positive performance review, or for other grievances.

In the other half of the cases, the insider was motivated by financial gain (28%) or competitive business advantage (22%). This explains why this subset of insiders targeted the IP of the victim organization. Recognition, curiosity, or ideology also played a cumulative role in 18% of the 50 cases involving TBPs in individual relationships.

Case Summaries: TBP Insiders with an Individual Relationship

In the sample cases summarized below, the insiders are from a TBP who had an individual relationship with the victim organization.

1. The insider had been contracted through the TBP to work on the IT staff of a telecommunications company but was terminated for poor performance. After his termination, he used his company-issued laptop to access the victim organization's network and used a shared password, which had not been changed since his departure, to access user accounts. The insider was caught when an employee at the victim organization noticed her last login was time stamped only a few hours previously, a time at which she was not logged into the system. This led to an investigation of the logs, which discovered the insider's actions.

[5] Note that the crime presented in Scenario II fits the pattern of the typical insider IT sabotage attack, regardless of whether the insider is an employee or a TBP. ***Insider IT sabotage*** is an insider's use of IT to direct specific harm at an organization or an individual. Examples include the malicious deletion of organizational information, bringing down organizational systems, and website defacement to embarrass the organization [Moore 2008].

2. The insider was a software development consultant for an IT company. The insider wanted a share of the company, which he demanded over the course of a year. The victim organization refused the insider's request and gave him a 3-month notice of the termination of his contract. The insider logged into the system, deleted files, and blocked access to the company's system until his demand was met. The company reported the insider to the FBI, who arrested the insider.
3. The insider was hired through the TBP as a temporary helpdesk agent and network technician in the customer support department of an IT company. The insider wanted to be hired as a full-time employee but was informed he would be terminated. As a result, the insider wrote several threatening emails, which led to his immediate termination. In retaliation, the insider used his remote access channels to access the victim organization's network, change administrative passwords, remove network access to systems, delete event logs, and modify the accounts of people involved with his termination.
4. The insider was a systems administrator for a TBP that was a contractor to a government agency. The insider's supervisor reprimanded him for frequent tardiness, absence, and unavailability for work. The insider planted a logic bomb on the government organization's server to delete critical files. The insider attempted to conceal his activities by removing history files, creating malicious code to overwrite itself after execution, and framing his supervisor for the malicious act. The insider was caught after arousing suspicion by constantly calling the victim organization to check on the system servers after his termination. Fortunately, the logic bomb never executed.
5. The insider, a temporary bank employee, was responsible for processing large cash deposits and placing them in the vault in bank-issued deposit bags. On-site and during work hours, the insider created fake deposit bags using the company-issued system, put them in the vault in the place of legitimate deposit bags, and stole the money with the legitimate deposit bags. In total, she stole more than $92,000 during a 3-month period. Even though each of the 12 customers complained of their deposits not being credited to their accounts, it was not until the 12th customer's complaint that the organization investigated and discovered the insider's scheme using surveillance footage and transaction logs.
6. The insider was a former IT contractor with a pharmaceutical company. After a dispute with senior management, the insider resigned. Sometime prior to his attack, the insider used his home network to install a piece of software on the victim organization's server. The insider used a restaurant's internet connection and a user password that had not yet been deactivated to access the victim organization's server. Then the insider used the previously installed piece of software to delete virtual machines that hosted the organization's email, order tracking, and financial management systems. This halted the organization's operations for several days. The insider's connection to the attack was discovered via his purchases in the restaurant near the time of the attack.

Summary Observations

Table 1 displays the statistics of observed cases for TBP insiders categorized by organizational relationships and individual relationships. It also compares TBP insider cases with our larger corpus of traditional insider cases.[6] As explained in this article, there are a few notable differences in the risks exploited based on the type of relationship an insider has with the victim organization.

Table 1: Comparison of Organizational TBPs, Individual TBPs, and Regular (Non-TBP) Insiders

	Trusted Business Partner		Non-TBP Insider
	Organizational	Individual	
Type of Position			
Technical	**45%**	**80%**	**39%**
Nontechnical	**55%**	**20%**	**61%**
Authorized Access			
Authorized Access	**44%**	**36%**	**48%**
Unauthorized Access	**26%**	**36%**	**23%**
Location			
On-Site	**81%**	**60%**	**73%**
Remote Access	**19%**	**40%**	**27%**
Employment Status			
Current	**90%**	**69%**	**76%**
Former	**10%**	**31%**	**24%**
Type of Insider Crime			
Fraud	**64%**	**23%**	**54%**
Theft of Intellectual Property	**28%**	**18%**	**19%**
Sabotage	**8%**	**59%**	**27%**
Motive for Insider Crime			
Financial Gain	**59%**	**28%**	**53%**
Revenge	**0%**	**46%**	**21%**
Business Advantage	**15%**	**22%**	**35%**
Recognition, Curiosity, or Ideology	**19%**	**18%**	**8%**
Other	**15%**	**14%**	**10%**

Note: Because some cases had missing data points, varying levels of unknown values were found within each of the categories listed within the table. The statistics presented in this table represent the cases for which the two corresponding variables (i.e., TBP type and employment status) were known. Additionally, some insiders had multiple motives, which explains why this category has a sum greater than 100% for each type of insider.

These summary statistics point to a key pattern of TBPs with individual relationships. In contrast to organizational TBPs and regular insiders, TBPs with individual relationships seem much more likely to hold a technical position, conduct an act of sabotage motivated by revenge, and often use

[6] At the time of this report's publication, there are 448 cases in our database where the subjects were strictly non-TBP domestic insiders.

remote access to achieve their goal. Organizational TBPs, on the other hand, seem to be primarily motivated by financial gain, which is why they are more likely to conduct fraud than individual TBPs and regular insiders. One final interesting observation is that TBPs in general are slightly more likely to be motivated by recognition, curiosity, or ideology than traditional insiders. The actionable interpretation of this finding is left to the reader, though our own working hypothesis is that TBPs often have a diminished sense of loyalty to the victim organizations, allowing other motivators (personal reputation, organizational transparency, association to the internet underground, etc.) to prevail.

TBP cases are similar to insider threat cases not involving TBPs. This finding agrees with the findings in *The CERT® Guide to Insider Threats*, which elaborates on TBP cases versus non-TBP cases [Cappelli 2012]:

The only difference is that the insider worked for a trusted business partner, rather than at the victim organization. Note how this situation complicates the mitigation strategy for this type of case! If the victim organization performed [the function contracted to the TBP] in-house, it could design its business processes to mitigate this threat, and implement auditing controls to detect any malfeasance….

The bottom line is that while it might appear that outsourcing business functions will result in cost savings, be sure to factor in the insider threat risk from your new "insiders" at the TBP before making your final decision.

Organizations wishing to enlist the help of TBPs must recognize their inherent differences from regular employees. Most TBPs have different motives, loyalties, goals, and skill sets, which result in different behavioral trends. An awareness of these trends can allow employees in various levels of an organization to appropriately and effectively utilize TBPs to achieve the organization's mission while minimizing the potential risks posed by this unique type of insider.

Recommendations for Mitigation and Detection of the Insider Threat from TBPs

This section summarizes a set of recommendations for organizations concerned about malicious acts by employees of TBPs [Cappelli 2008].

Recommendation 1: *Understand the policies and procedures of the trusted business partner.*

An organization establishes policies and procedures to protect its assets and achieve its mission. However, when an organization considers enlisting the support of a TBP, it should ensure that the TBP's policies and procedures are at least as effective as its own safeguards. This includes physical security, staff education, personnel background checks, security procedures, termination, and other safeguards.

Recommendation 2: *Monitor intellectual property to which access is provided.*

When organizations establish an agreement with a TBP, they also need assurance that the IP they provide access to is protected. Organizations need to ensure that access to and distribution of this data are monitored. Organizations should verify there are mechanisms for logging the dissemination of data. Organizations should be aware of the TBP's procedures to investigate possible disclosure of their information.

Recommendation 3: *Maintain access rights management.*

When contracting with a TBP to handle sensitive data, it is important for the organization to know how data is going to be managed. In a number of cases, the TBP could not handle the full workload it took on and subcontracted to another organization or brought in temporary employees to process the job. The organization should be aware of these arrangements and ensure the data will be handled by acceptable means.

Recommendation 4: *Understand the personnel policies and procedures of the trusted business partner.*

When contracting with a TBP, the organization should insist that the partner organization investigate and clear its own employees in ways commensurate with the organization's own procedures. In a few cases in the CERT insider threat database, the TBP employed workers with criminal backgrounds or connections to the internet underground. Organizations should not compromise their level of security to have a job accomplished faster.

Recommendation 5: *Anticipate and manage negative workplace issues.*

When an organization decides to hire consultants, contractors, or temporary employees, the organization should make them aware of the organization's policies and practices for acceptable work behavior. Negative workplace issues have been known to trigger illicit insider activity; it is important that policies and procedures for managing such events consider permanent employees, contractors, consultants, and temporary employees. It is also important that organizations do not provide false hope for these employees regarding their likelihood of being hired more permanently. If a company has indicated they may hire a contractor or consultant full time but then decides not to do so, it should perform an assessment of the individual's insider risk. The organization should remove the individual's access and change any account passwords shared by the individual to mitigate risks before it informs the individual that he or she will not be hired. It has proven risky to retain the services of disappointed or disgruntled temporary workers.

Recommendation 6: *Deactivate access following termination.*

When an employee, consultant, or contractor is terminated or suspended, all of that individual's access should be disabled. When organizations are forming an agreement with a TBP, they should make certain the TBP performs rigorous termination procedures as well. In a number of cases

involving contractors, access was not disabled immediately after termination, and the insider was able to exploit that access in the commission of their crime.

Recommendation 7: *Enforce separation of duties.*

A number of insiders exploited the capability to perform certain actions in such a way that circumvented normal separation-of-duties controls. Business processes should enforce separation of duties, regardless of the speed or priority required. While different levels of controls may be associated with tasks of different priority, processes should not be left without protections against possible exploitation by a disgruntled or greedy insider.

Recommendation 8: *Create contractual agreements that make it clear the trusted business partner is also responsible for protecting organizational resources.*

Contracts with a TBP should include restrictions on how the TBP handles and shares the organization's information. This should include restrictions on the TBP's ability to subcontract with other organizations on tasks involving sensitive information. There should be standard terms and conditions that allow the organization to apply the same policies and procedures to contractors, subcontracts, and consultants that it applies to its own employees, including mandatory flow-down provisions from primary contractors to subcontractors. Also, contracts should include notification requirements for breaches and termination of employees working on the contract. The contracting organization should make its security requirements clear and also develop consequences that will incentivize the TBP to protect key resources.

About the Insider Threat Center

The CERT Insider Threat Center is part of the Enterprise Threat and Vulnerability Management (ETVM) team in the CERT Program. The ETVM team helps organizations improve their security posture and incident response capability by researching technical threat areas; developing information security assessment methods and techniques; and providing information, solutions, and training for preventing, detecting, and responding to illicit activity. ETVM team members are domain experts in insider threat and incident response, and team capabilities include threat analysis and modeling; development of security metrics and assessment methodologies; and creation and delivery of training, courses, and workshops. Our insider threat database allows us to examine broad and specific trends.

For additional information regarding the content of this article or other research conducted at the CERT Insider Threat Center, please contact Dawn Cappelli (dmc@cert.org) or Randy Trzeciak (rft@cert.org).

References

URLs are valid as of the publication date of this document.

[Burke 2009]
Burke, Brian E. & Christiansen, Christian A. *Insider Risk Management: A Framework Approach to Internal Security*. Interactive Data Corporation (IDC), 2009.
http://www.rsa.com/solutions/business/insider_risk/wp/10388_219105.pdf

[Cappelli 2008]
Cappelli, D. M.; Moore, A. P.; Shimeall, T. J.; & Trzeciak, R. F. *Common Sense Guide to Prevention and Detection of Insider Threats: 3rd Edition*. Software Engineering Institute, Carnegie Mellon University, CyLab, and the Internet Security Alliance, 2008.

[Cappelli 2012]
Cappelli, D. M.; Moore, A. P.; & Trzeciak, R. J. *The CERT® Guide to Insider Threats*. Addison-Wesley, 2012.

[Moore 2008]
Moore, A. P.; Cappelli, D. M.; & Trzeciak, R. F. "The 'Big Picture' of Insider IT Sabotage Across U.S. Critical Infrastructures," 5-17. *Insider Attack and Cyber Security: Beyond the Hacker*, Springer Science+Business Media, 2008.

[Moore 2009]
Moore, A. P.; Cappelli, D. M.; Caron, T.; Shaw, E.; & Trzeciak, R. F. "Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model." *Proceedings of the 1st International Workshop on Managing Insider Security Threats (MIST 2009)*, Purdue University, West Lafayette, IN, USA, June 16, 2009.
http://www.cert.org/insider_threat/docs/Insider_Theft_of_IP_Model_MIST09.pdf

[U.S. Census Bureau 2011]
U.S. Census Bureau. *The 2012 Statistical Abstract: Labor Force, Employment, & Earnings. Rep. no. 592 - Civilian Labor Force-Percent Distribution by Sex and Age*. U.S. Census Bureau, 2011.
http://www.census.gov/compendia/statab/2012/tables/12s0592.pdf

[U.S. Secret Service 2010]
U.S. Secret Service. *Criminal Investigations*. U.S. Secret Service, 2010.
http://www.secretservice.gov/criminal.shtml